DUMPSARENA

GIAC Certified Firewall Analyst

GIAC GCFW

Version Demo

Total Demo Questions: 15

Total Premium Questions: 391

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	143
Topic 2, Volume B	248
Total	391

QUESTION NO: 1

Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead-space?

A. Network Intrusion Detection System (NIDS)

B. Host Intrusion Detection System (HIDS)

C. Biometric device

D. Man trap

ANSWER: D

QUESTION NO: 2

You run the tcpdump command line utility and get a report produced by tcpdump. What information does this report include?

Each correct answer represents a complete solution. Choose three.

A. Packets dropped by kernel

B. Packets discarded

C. Packets captured

D. Packets received by filter

ANSWER: A C D

QUESTION NO: 3

The simplest form of a firewall is a packet filtering firewall. A packet filtering firewall filters packets at the Network layer and Transport layer. What are the types of information that are filtered at the Network layer of the OSI reference model?

Each correct answer represents a complete solution. Choose all that apply.

A. TCP/IP protocols

B. TCP control flags

C. IP addresses

D. TCP and UDP port numbers

ANSWER: A C

QUESTION NO: 4

Distributed Checksum Clearinghouse (DCC) is a hash sharing method of spam email detection.

Which of the following protocols does the DCC use?

A. ICMP

B. TELNET

C. UDP

D. TCP

ANSWER: C

QUESTION NO: 5

Which of the following wireless security policies helps to prevent the wireless enabled laptops from peer-topeer attacks when the laptops are used in public access network?

A. Use protocol analyzer

B. Use Port Address Translation

C. Use security protocols

D. Use firewall

ANSWER: C D

QUESTION NO: 6

Sam works as a Security Manager for GenTech Inc. He has been assigned a project to detect reconnoitering activities. For this purpose, he has deployed a system in the network that attractsthe attention of an attacker. Which of the following rulebases will he use to accomplish the task?

A. Network Honeypot rulebase

B. Exempt rulebase

C. Backdoor rulebase

D. SYN Protector rulebase

ANSWER: A

QUESTION NO: 7

A Proxy firewall, also known as Application Gateway Firewall, filters information at which of the following layers of the OSI reference model?

Each correct answer represents a part of the solution. Choose all that apply.

A. Transport layer

B. Physical layer

C. Presentation layer

D. Application layer

ANSWER: A D

QUESTION NO: 8

Rick works as the Security Manager for TechPerfect Inc. He wants to continue the evaluation of rules according to the ordered list to identify matches even if a match is found. Which of the following rulebases will he use to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. IDP rulebase

B. Backdoor rulebase

C. Terminal rulebase

D. Nonterminal rulebase

ANSWER: A D

QUESTION NO: 9

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. You have searched all open ports of the we-are-secure server. Now, you want to perform the next information-gathering step, i.e., passive OS fingerprinting. Which of the following tools can you use to accomplish the task?

A. NBTscan

B. Nmap

C. P0f

D. Superscan

ANSWER: C

QUESTION NO: 10

You work as a Network Administrator for a bank. For securing the bank's network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network.

After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed. What type of response is the IDS giving?

A. False Negative

B. True Negative

C. True Positive

D. False Positive

ANSWER: A

QUESTION NO: 11

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN.

What steps can be used as a countermeasure of ARP spoofing?

Each correct answer represents a complete solution. Choose all that apply.

A. Using ARP Guard utility

B. Using smash guard utility

C. Using static ARP entries on servers, workstation and routers

D. Using ARP watch utility

E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

ANSWER: A C D E

QUESTION NO: 12

You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following would be most helpful against Denial of Service (DOS) attacks?

A. Stateful Packet Inspection (SPI) firewall

B. Packet filtering firewall

C. Network surveys.

D. Honey pot

ANSWER: A

QUESTION NO: 13

You work as a Firewall Analyst in the Tech Perfect Inc. The company has a Linux-based environment. You have installed and configured netfilter/iptables on all computer systems.

What are the main features of netfilter/iptables?

Each correct answer represents a complete solution. Choose all that apply.

A. It includes many plug-ins or modules in 'patch-o-matic' repository

B. It includes a number of layers of API's for third party extensions

C. It offers stateless and stateful packet filtering with both IPv4 and IPv6 addressing schemes

D. It provides network address and port address translations with both IPv4 and IPv6 addressing schemes

ANSWER: A B C

QUESTION NO: 14

Which of the following firewalls filters the traffic based on the header of the datagram?

A. Application-level firewall

B. Packet filtering firewall

C. Circuit-level firewall

D. Stateful inspection firewall

ANSWER: B

QUESTION NO: 15

An organization has a TCP/IP based network. It uses IPv6 addressing in its network. IPv6 tackles addressing and routing-table problems, and improves the protocol as well. Which of the following statements is true about IPv6?

A. It uses symmetric key encryption.

B. Its address is 32 bits in length.

C. It eliminates the primary need for Network Address Translation (NAT).

D. It implements broadcasting.

ANSWER: C